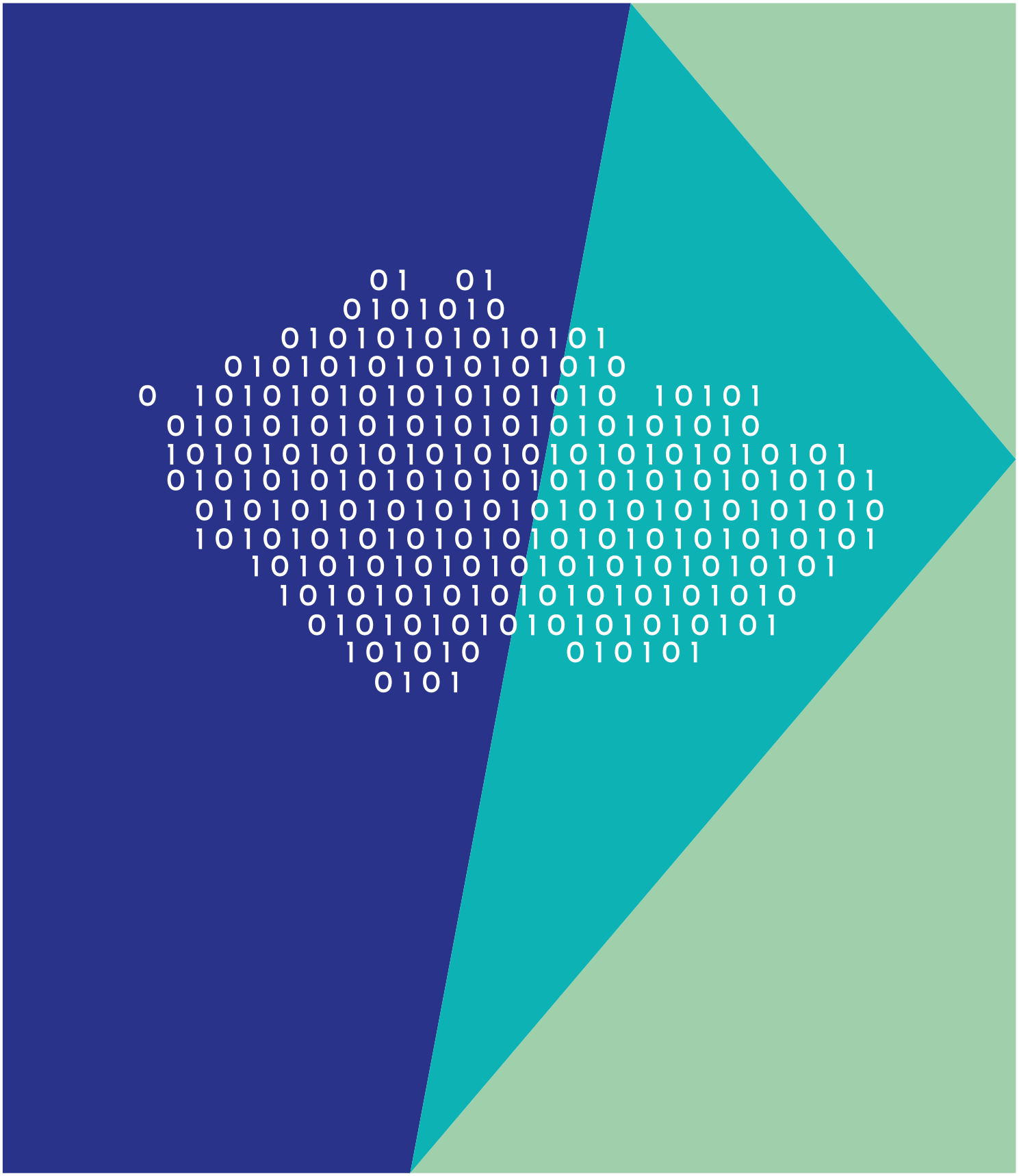
Národní politika kryptografické ochrany utajovaných informací v České republice

pro období let 2024 až 2030, s výhledem do roku 2040



Obsah

Seznam použitých zkratek

ČR	Česká republika
EU	Evropská unie
KIS	Komunikační a informační systémy
KOUI	Kryptografická ochrana utajovaných informací
KO	Kryptografická ochrana
KP	Kryptografický prostředek
NATO	Organizace Severoatlantické smlouvy
NP	Národní politika
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
UI	Utajovaná informace
ZoUI	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Manažerské shrnutí

Národní politika kryptografické ochrany utajovaných informací v České republice do roku 2030 s výhledem do roku 2040 (NP KOUI) je národním strategickým dokumentem zastřešujícím oblast kryptografické ochrany utajovaných informací (KOUI) v ČR.

Rámec rozvoje KOUI

NP KOUI formuluje rámec rozvoje všech oblastí KOUI do roku 2030 s výhledem do roku 2040 v podmínkách dynamického vývoje společnosti, proměňujícího se bezpečnostního prostředí, rapidního rozvoje informačních a komunikačních technologií a kryptologie. Jejím cílem je hledat nástroje a postupy, jak čelit rostoucím bezpečnostním hrozbám pro KOUI, včetně těch v oblasti kybernetické bezpečnosti.

Vize NP KOUI

Hlavní vizí NP KOUI je v rámci bezpečnostního systému České republiky (ČR) systematicky, cílevědomě a efektivně rozvíjená KOUI.

Strategické cíle

Strategické cíle NP KOUI požadují zajištění systematického rozvoje KOUI, zvýšení podílu národních kryptografických prostředků, zajištění vysoké úrovně služeb KOUI, předvídatelnost rizik pro KOUI a zvýšení informovanosti o KOUI.

Klíčové faktory úspěchu

Pro úspěšné naplnění definovaných strategických cílů je rozhodující zejména rozsáhlejší aktualizace právní úpravy KOUI a uvedení níže navrženého konceptu národního kryptografického prostředku pro národní komunikační a informační systémy (KIS) do systému KOUI. Kritickým faktorem pro naplňování NP KOUI je zajištění potřebných zdrojů, především lidských a finančních.

Implementace a zodpovědnost

Způsob naplnění strategických cílů a klíčové aktivity NP KOUI bude rozpracován v dokumentu Implementační plán politiky kryptografické ochrany utajovaných informací v České republice. V něm budou obsaženy konkrétní adresné a termínované úkoly. Garantem jeho zpracování je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Úvodní slovo ředitele NÚKIB

Bouřlivý rozvoj současných KIS, který zasahuje do všech oblastí společenského života, a jejich široká dostupnost v každodenním životě zvyšuje riziko napadení informací zpracovávaných v těchto systémech. KIS jsou tak permanentně vystavovány hrozbám (včetně kybernetických) a vlivům, které mají základ v dynamickém vývoji společnosti a proměňujícím se bezpečnostním prostředí ve světě, výsledcích vědeckého bádání a v nových informačních a komunikačních technologiích.

Ochrana utajovaných informací (UI) hraje zásadní roli při zajišťování bezpečnosti, ochrany zájmů ČR a při plnění mezinárodních závazků vyplývajících z členství v Evropské unii (EU) a Organizace Severoatlantické smlouvy (NATO). KOUI představuje nezpochybnitelnou a neopomenutelnou součást bezpečnostní politiky ČR. Proto je třeba stále větší pozornost věnovat zabezpečení těchto utajovaných informací před jejich kompromitací, obzvláště nyní během bouřlivého geopolitického vývoje. Věřím, že tato politika posílí důslednou ochranu utajovaných informací a tím i stabilitu a bezpečnost ČR v dynamicky se měnícím světě.

Ing. Lukáš Kintr
Ředitel Národního úřadu pro kybernetickou a informační bezpečnost

Směřování Národní politiky a pravidla

K tomu, aby KOUI bezpečně a spolehlivě plnila požadované funkce, musí být správně a srozumitelně stanoveno její směřování a potřebná realizační pravidla a opatření, včetně jejich dodržování a kontroly ve všech dílčích oblastech KOUI zahrnujících personální, fyzickou, administrativní, kryptografickou a provozně technickou stránku bezpečnosti. Zajištění všech těchto činností vyžaduje koordinované úsilí všech subjektů zúčastněných v zajišťování KOUI, od orgánů státu přes komerční subjekty až po jednotlivé pracovníky.

Cíl a zpracování

Základním cílem NP KOUI je systémově upravit rozvoj všech oblastí tvořících systém KOUI, z nichž každá má svou nezastupitelnou roli, a využít jejich provázanosti a součinnosti k následnému stanovení implementačních opatření pro rozvoj KOUI v ČR. Zpracování NP KOUI ukládá NÚKIB zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (ZoUI). Tento dokument představuje první zpracování NP KOUI a je určen pro období let 2024 až 2030, s výhledem do roku 2040.

Strategický význam

NP KOUI je vrcholovým strategickým dokumentem, který udává hlavní směry rozvoje KOUI a je východiskem pro zpracování navazujících dokumentů. Mezi hlavní cíle KOUI patří zajištění bezpečnosti UI pomocí přiměřených a odpovídajících opatření, která budou chránit UI tak, aby poskytovala odpovídající míru jistoty jejich uživatelům ve světle měnícího se prostředí. Naplnění cílů KOUI je proto nezbytné pro zajištění bezpečného provozu moderních KIS zpracovávajících UI. Úspěch KOUI záleží nejen na účinné aplikaci a vymáhání stávajících pravidel, ale zejména na jejich systematickém a účinném rozvoji.

Etapy tvorby

Tvorba NP KOUI probíhala ve dvou na sebe navazujících etapách. Předmětem první, analytické etapy, bylo zmapování a zhodnocení silných a slabých stránek stávajícího systému KOUI. Předmětem druhé, koncepční etapy, je pak definování strategických cílů a na ně navázaných klíčových aktivit a realizačních opatření, které budou předmětem samostatného implementačního dokumentu.

Struktura

NP KOUI se člení na analytickou a strategickou část, která obsahuje strategické cíle a klíčové aktivity k jejich realizaci.Při jejím zpracování byla zohledněna též Metodika přípravy veřejných strategií Ministerstva pro místní rozvoj ČR [19].

1 Základní východiska kryptografické ochrany utajovaných informací

KOUI stojí na několika základních východiscích. Systém KOUI se opírá o legislativní, organizační, kryptologické, provozně technické, administrativní a personální prvky. Každý z nich má v zabezpečení KOUI své nezastupitelné místo a výsledná úroveň zabezpečované KOUI je dána úrovní nejslabšího prvku.

Použití kryptografických metod umožňuje bezpečné a rychlé předávání UI v KIS. Rovněž umožňuje bezpečné uložení UI na nosič informací, se kterým je pak možno nakládat jako s UI nižšího stupně, případně jako s neutajovanou informací.

Prolomení kryptografické ochrany znamená ve svém důsledku újmu na chráněných zájmech ČR, proto je nutné věnovat zajištění celého systému KOUI mimořádnou pozornost.

1.1 Právní strategický rámec

Směřování a naplňování NP KOUI významně ovlivňuje řada legislativních a strategických materiálů na národní úrovni a na úrovni EU a NATO.

Národní strategický a právní rámec

Strategie	Bezpečnostní strategie České republiky 2023 [12] Obranná strategie České republiky 2023 [13]
Zákonné předpisy	ZoUI[1] [3]
Podzákonné předpisy	Vyhláška o provádění certifikace při zabezpečování KOUI [6] Vyhláška o zajištění KOUI [8] Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků [7] Vyhláška o administrativní bezpečnosti a o registrech UI [9] Vyhláška o bezpečnosti KIS a dalších elektronických zařízení nakládajících s UI a o certifikaci stínících komor [5]

Nadto vydal NÚKIB, jakožto národní bezpečnostní autorita pro oblast KOUI, řadu bezpečnostních standardů[2], jež dále upravují bezpečnostní způsobilost kryptografických prostředků (KP) a procesy zajištění KOUI v ČR.

Strategický a právní rámec EU a NATO

EU	Rozhodnutí Rady EU ze dne 23. září 2013, o bezpečnostních pravidlech na ochranu utajovaných informací EU, 2013/448/EU [14] Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti, Rada Evropské unie, 7371/22, Brusel 21. března 2022 [15]
NATO	Security within the North Atlantic Treaty Organisation (NATO), C-M(2002)49-REV1 [16] NATO 2022 Strategic Concept, NATO Summit in Madrid, 29 June 2022 [17]

1 Na KOUI lze pohlížet dvěma způsoby podle rozsahu jejího pojetí, kde **širokým pojetím** se rozumí KOUI v rozsahu ZoUI se zohledněním zákona o kybernetické bezpečnosti (ZKB) [4] a **úzkým pojetím** pak KOUI jen v rozsahu ZoUI. KOUI v NP KOUI je pojímána v úzkém pojetí.

2 **Bezpečnostní standard** ve smyslu ZoUI je utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací.

2

Trend vývoje v oblasti KOUI a hodnocení současného stavu v ČR

Základem pro stanovení směřování NP KOUI je poznání nynějšího stavu všech oblastí KOUI, trendů jejich vývoje a identifikace problémů a nedostatků.

2.1 Trendy rozvoje v oblasti KOUI

Současný stav zajištění KOUI je výrazně ovlivněn probíhajícími společenskými a technologickými změnami (výsledky vědeckého bádání, zejména v oblasti kryptologie či poznatky nových informačních a komunikačních technologií) i rychle se měnícím bezpečnostním prostředím ve světě.

Kryptoanalýza[3] a důvěra v kryptografii

Od moderních kryptografických algoritmů aplikovaných v prostředcích KOUI se očekává, že odolají kryptoanalytickým útokům. Důvěra v jejich bezpečnost je průběžně budována konsensem nad tím, jaké algoritmy odolávají všem známým kryptoanalytickým útokům. Přesto prolomení kryptografických algoritmů nelze z krátkodobého, a především z dlouhodobého hlediska zcela vyloučit.

Přínos a problémy nových hardwarových technologií

Hardwarové technologie použité v KP prošly během uplynulých let výraznými změnami. Pro aktivní součástkovou základnu je charakteristický zejména velký výpočetní výkon, který spolu s paměťovou kapacitou umožňuje rychle zpracovávat velké objemy dat. Implementace speciálních bezpečnostních funkcí, včetně kryptografických, se stávají jejich nedílnou součástí. V současné době lze s použitím obvodů, jako jsou procesory a hradlová pole nových generací, efektivně vytvářet KP a jeho dílčí moduly s velikou složitostí.

Nové hardwarové technologie jsou charakteristické těmito znaky:

Integrace a miniaturizace	Vysoký stupeň integrace a miniaturizace provedení a další provozní vlastnosti výrazně ovlivňují výkonové vlastnosti a finální provedení vyvíjených zařízení.
Vysoká funkční spolehlivost	Funkční spolehlivost dnešní součástkové základny používané v bezpečnostním hardwaru je na poměrně vysoké úrovni. Případná nespolehlivost nastává zpravidla, pokud hardwarová součástka vyráběná dvěma výrobci má u jednoho výrobce plnou funkcionalitu dle popisu a u druhého výrobce je funkcionalita omezena jen na nejčastěji používané funkce, případně pokud součástka není funkčně spolehlivá v celém pásmu definovaných hraničních podmínek provozování.
Složitost a riziko „zadních vrátek“	Vysoká míra složitosti současně umožňuje vytvářet předpoklady pro aplikaci speciálních funkcí, jež jsou známy jen jejímu návrháři a nejsou uvedeny v popisu součástky. Použití takové součástky v návrhu hardwaru KP s sebou přináší riziko vzniku „zadních vrátek“ pro únik UI a dalších chráněných aktiv nebo ovlivňování jejich funkční spolehlivosti.

[3] **Kryptoanalýza** je disciplína zabývající se analýzou šifrovaných textů s cílem zjistit původní nezašifrovanou zprávu nebo získat informace o použité šifře. Jedná se o odvětví kryptologie, jež si klade za cíl porozumět, prolomit a narušit šifrovací techniky a metody, a tak získat neoprávněný přístup k zašifrovaným informacím.

Aplikace umělé inteligence[4] v kryptologii

Metody umělé inteligence lze aplikovat na kryptografické problémy různými způsoby a jejich cílem je podrobněji porozumět jednak potenciálním útokům, jednak bezpečnostním garancím kryptografických metod a implementací, což může přispět k posílení bezpečnostních či obranných mechanismů.

Konkrétně může být umělá inteligence použita k podpoře vytváření bezpečnostních důkazů[5] nebo k odhalení chyb v prováděných bezpečnostních důkazech, ale zároveň i ke zvýšení efektivity nebo automatizaci útoků.

Matematická kryptoanalýza

Matematická kryptoanalýza se zabývá problémem prolomení kryptografických algoritmů a schémat využitím jejich matematických vlastností. Současné kryptografické algoritmy a schémata jsou sice typicky odolné proti všem známým útokům tohoto typu, nelze však vyloučit nalezení zcela nového útoku v budoucnu. Identifikace potenciálních zranitelností kryptografických algoritmů a schémat již v rané fázi jejich návrhu probíhá také díky výzkumu nových metod útoků.

Ekonomické možnosti

Aktuálně prováděné restrikce veřejných rozpočtů obecně výrazně omezují možnosti zajišťování KO ČR, zejména s ohledem na zajištění vývoje, obměny, pořizování nových, údržby a servisu aktuálních KP a souvisejícího materiálu, které jsou potřebné pro zajištění KO v KIS.

Na druhé straně zostřená mezinárodní situace a závazky v rámci NATO si již vyžádaly navýšení rozpočtu na obranu v roce 2024 a jeho navyšování v dalších letech.

S ohledem na skutečnost, že KO tvoří nedílnou součást obranných technologií, především těch komunikačních, lze důvodně očekávat, že část těchto finančních prostředků bude také směřována do rozvoje KO.

---

4 **Umělá inteligence** v kryptologii zahrnuje využívání technik a nástrojů umělé inteligence, zejména tzv. strojového učení, které může vést ke zlepšení bezpečnostních postupů, analýzy dat a prevence kybernetických útoků. V rámci strojového učení se počítače učí z dostupných dat a zlepšují se s přibývajícími zkušenostmi z reálného prostředí, aniž by byly explicitně programovány.

5 **Bezpečnostní důkaz** je matematický argument nebo analýza, která má za cíl demonstrovat bezpečnost kryptografického protokolu, algoritmu nebo šifrovací metody. Bezpečnostní důkazy jsou klíčovým nástrojem pro posuzování odolnosti kryptografických schémat proti různým druhům útoků.

Aktuální trendy v kryptologii

V oblasti kryptologie, která hraje klíčovou roli v zajišťování KOUI, lze identifikovat nové výzvy a významné trendy, které vychází zejména z technologického vývoje.

Hrozba postranních kanálů

Výrazný rozvoj nových technologií současně umožnil rozvoj analýzy postranních kanálů, které se oproti konvenčnímu matematickému přístupu nesoustředí na slabá místa implementovaného kryptografického algoritmu, ale na časové, elektromagnetické, proudové, chybové, akustické a jiné informace, které unikají z implementace kryptografického algoritmu do informačních technologií při jeho běhu.

Kvalitní generátory náhodných čísel

Generování náhodných posloupností tvoří významnou bezpečnostní část v procesu kryptografické ochrany, kde jsou využívány pro vytváření kryptografických klíčů a dalších náhodných bezpečnostních parametrů. K tomu, aby byl takový generátor hodnocen jako kvalitní, musí obsahovat zdroj kvalitní náhody, který bude garantovat funkční stabilitu a ve výsledku vytvářet nepředvídatelnou posloupnost s dobrými statistickými vlastnostmi. Hledání takových zdrojů náhody a metod testování náhodnosti je věnována významná pozornost ze strany bezpečnostní komunity.

Přechod ke kvantově odolné kryptografii

Průlomy ve výpočetní technice, jako je vznik kvantových počítačů nebo nový přístup ke klasické kryptoanalýze, mají potenciál podkopat předchozí předpoklady o síle kryptografických algoritmů, a tím i ochranu poskytovanou zašifrovaným datům. Hrozba budoucích tzv. kryptograficky relevantních kvantových počítačů již podnítila přípravy na přechod na nové, kvantově odolné algoritmy veřejného klíče. Jedná se o tzv. postkvantovou kryptografii (Post-Quantum Cryptography, PQC). V současné době jsou již známy dílčí výsledky soutěže (organizované Národním institutem pro standardy a technologie (NIST) Spojených států amerických) na vytvoření doporučených algoritmů, fungujících na nových principech pro výměnu klíčů, šifrování a digitální podpisy, které jsou odolné vůči útokům kvantových počítačů. Tyto dílčí výsledky mohou urychlit implementaci daných algoritmů.

Kvantově odolné technologie pro informační bezpečnost

Rozvoj kvantových technologií se nezaměřuje jen na „prolomení“ aktuálních kryptografických algoritmů, jejichž odolnost je postavena na výpočetní složitosti. Současně také přináší nové vlastní přístupy k řešení ochrany informací v KIS, které jsou odolné proti kvantovým počítačům. Jedním z takových řešení je komunikace založená na kvantové distribuci klíče (Quantum Key Distribution, QKD), ve které se sdílené kryptografické klíče účastníků komunikace distribuují ve formě stavů kvantových fotonů právě optickým kvantovým kanálem, odolným proti odposlechům a duplikování.

Budoucí hrozba pro shromážděná šifrovaná data[6]

Subjekty používající KO očekávají, že šifrování ochrání zpracovávané informace před potenciálním útočníkem, který má přístup k jejich zašifrované podobě. V tomto případě musí být šifrování zabezpečeno proti současným i budoucím dešifrovacím schopnostem útočníka. Proto poskytnutí bezpečnostních záruk znamená vytvoření předpokladů o síle kryptografických algoritmů proti budoucím kryptoanalytickým útokům a předpovědí o možnostech výpočetního výkonu pro potřeby prolomení KO.

Mimořádné situace a bezpečnostní incidenty

KOUI je v dnešní době ohrožována mnoha nestandardními událostmi, které mohou narušit její zajištění a v důsledku tak ohrozit bezpečnost chráněné UI.
Mimořádné události ve smyslu zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů [1], a obdobné jevy sice nemusí být přímo směřované na narušení KOUI, avšak v jejich důsledku může dojít k ohrožení nebo přímo narušení KOUI, a tím i chráněné UI. Naproti tomu události označované jako bezpečnostní incidenty již přímo souvisí s KOUI a jejich výsledkem je úmyslné nebo neúmyslné narušení KOUI.

2.2 Hodnocení současného stavu KOUI

Výchozím podkladem NP KOUI pro hodnocení současného stavu je utajovaný dokument Analýza stavu kryptografické ochrany utajovaných informací v České republice 2023 [11] zpracovaný NÚKIB.

V dokumentu jsou detailně posouzeny oblasti lidských a materiálových zdrojů v KO, pracoviště v KO, KO v KIS a rozvoj kryptologie a výroba KP. Pro každou z uvedených oblastí jsou prostřednictvím tabulky SWOT[7] analýzy identifikovány nejvýznamnější silné a slabé stránky, příležitosti, hrozby a stanovení jejich priorit a vyhodnocení.

---

6 **Strategie retrospektivního dešifrování** „Harvest now, decrypt later“ („sbírej teď, dešifruj později“) spočívá v získávání a dlouhodobém uchovávání v současnosti nečitelných zašifrovaných dat s očekáváním možného průlomu v technologii dešifrování, který by tato data v budoucnu učinil čitelnými.

7 Název je odvozený ze slov Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti) a Threats (hrozby).

3

Vize a základní strategické směřování NP KOUI

Vizí NP KOUI je kontinuálně, systematicky, cílevědomě a efektivně rozvíjená KOUI v ČR, která vychází ze základního strategického směřování ČR, NATO a EU, je integrální součástí bezpečnostního systému ČR a pružně reaguje na aktuální hrozby.

3.1 Poslání, hodnoty a principy KOUI

Posláním KOUI je zajištění ochrany UI na úrovni orgánů státu, právnických a fyzických osob a mezi nimi navzájem systémem opatření na ochranu UI s použitím kryptografických metod a kryptografických materiálů při jejím zpracování, přenosu nebo ukládání.[8]

K tomu, aby KOUI plnila své poslání, musí být postavena na těchto obecně platných principech:

1.

Aplikace bezpečné kryptografie

Požadovaná úroveň ochrany UI prostřednictvím KP musí být zajištěna bezpečnou implementací odolných kryptografických algoritmů a schémat.

2.

Důvěryhodnost KOUI

KOUI musí být vybudována a dále rozvíjena na pevných základech, cílevědomě a nezpochybnitelným způsobem. Důvěryhodnost je chápána jako vlastnost KOUI zajistit aktuálně i v budoucnu její soulad se stanovenými požadavky.

3.

Kvalita lidských zdrojů v KOUI

Lidské zdroje se podílí na významné části zajišťovaných činností v KOUI. Právě jejich bezpečnostní a odborná způsobilost spolu se s účinnou systematickou aplikací mechanismů řízení lidských zdrojů jsou zárukou zajištění profesionality KOUI.

4.

KOUI budovaná jako systém

Systematické budování, implementace a údržba struktury sloužící k zajištění bezpečnosti UI skrz KO. Daný systém by měl být rozvíjen jako organický celek.

5.

Systematické vyhodnocování rizik

Proces sloužící k identifikaci, analýze a hodnocení potenciálních hrozeb a zranitelností spojených s provozem nebo činnostmi v oblasti KOUI.

[8] § 5 písm. f) ZoUI.

3.2 Strategické cíle do roku 2030

K naplnění své vize definuje NP KOUI strategické cíle. Ty se zaměřují na zajištění bezpečného a kvalitativně se zlepšujícího systému KOUI. Uvažovaný systém odráží reálné potřeby a zohledňuje dynamicky měnící se svět technologií a změny globálního prostředí. Ve vztahu k rozvoji KP je výhled NP KOUI zaměřen až do roku 2040. Tyto cíle zahrnují:

1.

Zajistit systémový rozvoj KOUI

KOUI musí být zajišťována a rozvíjena jako organický celek při zohlednění všech jeho částí a vztahů mezi nimi. V souladu s dlouhodobou strategií rozvoje KOUI, která umožňuje reagovat na výzvy plynoucí z měnících se informačních technologií a bezpečnostního prostředí, je potřebné zajistit, aby byla přijatá opatření v KOUI optimální a provázaná.

2.

Zvětšit podíl národních KP na zajišťování KOUI

Zajištění KOUI v národních KIS národními KP, které má ČR plně pod kontrolou, představuje nezpochybnitelnou část bezpečnostního systému ČR v oblasti ochrany UI.
Cílovým stavem je nastavení rámce řešení národních KP, stanovení motivačních přístupů a vytvoření předpokladů pro výraznější použití národních KP v KOUI.

3.

Zajistit vysokou úroveň služeb KOUI

Udržení vysoké úrovně KOUI lze chápat jako kontinuální a nikdy nekončící proces, postavený na průběžném zdokonalování všech dílčích oblastí KOUI. Každá z těchto oblastí má nezastupitelné místo, avšak výsledná úroveň zabezpečované KOUI je dána úrovní jejího nejslabšího článku.
Cílovým stavem jsou nastavené procesy permanentního vyhodnocování a řízení rizik, kterým je KOUI průběžně vystavována.

4.

Zajistit předvídatelnost rizik ovlivňující KOUI

Prevence rizik v KOUI musí zohledňovat požadavky na zajištění dlouhodobé udržitelnosti vyžadované funkčnosti a bezpečnosti KOUI.
Cílovým stavem je nastavit systém, kdy na základě monitoringu rozvoje budou přijímána včasná opatření, která zajistí potřebnou úroveň KOUI.

5.

Zvýšit informovanost o možnostech a přínosu KOUI

Dostupnost a aktuálnost relevantních informací mají při zajišťování KOUI nezastupitelné místo. Přitom důležitým požadavkem na informace musí být zajištění harmonizace s příslušnými předpisy EU a NATO.
Cílovým stavem je vytvoření prostředí motivujícího k používání KOUI, kterou bude využívající subjekt chápat jako službu, jež mu pomáhá, je uživatelsky přívětivá a má zájem ji aktivně používat.

3.3 Nástroje k uplatňování a prosazování Národní politiky

Nástroje k uplatňování a prosazování NP KOUI zahrnují:

Právní nástroje

V rámci současné právní úpravy je aplikována zásada účelného rozdělení této problematiky zejména do obecně závazných právních předpisů, vyhlášky o zajištění KOUI [8] a vyhlášky o provádění certifikace při zabezpečování KOUI [6] a do bezpečnostních standardů vydávaných NÚKIB. Právní předpisy, které se zajištěním KOUI souvisejí nebo se na ně odkazují, zahrnují správní řád [2], vyhlášku o fyzické bezpečnosti a certifikaci technických prostředků [7], vyhlášku o bezpečnosti informačních a komunikačních systémů a certifikace stínicích komor [5] a vyhlášku o administrativní bezpečnosti a o registrech utajovaných informací [9].

Personální nástroje

Účelem personálních nástrojů je zajistit personální stabilizaci stávajících i nových pracovníků a jejich odpovídající ohodnocení. Další rozvoj KOUI je závislý právě na pracovnících, kteří splňují bezpečnostní a odborné požadavky. Významnou roli v tomto hrají motivační prvky (informovanost, otevřená komunikace se zpětnou vazbou, profesní růst, finanční a sociální bonusy aj.) či jiné formy uznání za přínos k rozvoji KOUI.

Ekonomické nástroje

Účelem ekonomických nástrojů je zajistit financování akvizic nových KP, financování projektů výzkumu, vývoje a inovací v kryptologii a zajištění kvalifikovaných pracovníků. Ekonomické nástroje současně zahrnují opatření směřující k přerozdělování lidských a věcných zdrojů (KP, pracoviště aj.).

Míra využití ekonomických nástrojů je podmíněna aktuálními možnostmi státního rozpočtu ČR. Další možností je financování rozvoje KOUI z prostředků EU. V případě vývoje KP se zdrojem mohou stát i odvozené výstupy pro použití v KIS podléhajících ZKB [4].

Institucionální nástroje

Účelem institucionálních nástrojů je zajistit procesy ve sdílení informací a nastavení opatření tak, aby se všechny zainteresované subjekty aktivně podílely na jejich prosazování. Nedílnou součástí institucionálního ukotvení jsou též kontrolní mechanismy. Současná KOUI zahrnuje NÚKIB jako gestora pro tuto oblast a další státní orgány a právnické osoby.

Pro potřeby prezentace, shromažďování, hodnocení a sjednocování stanovisek zainteresovaných subjektů k řešení podstatných problémů v rozvoji KOUI se jako vhodné a účinné ukazují nástroje oblasti spolupráce a sdílení informací.

Administrativní nástroje

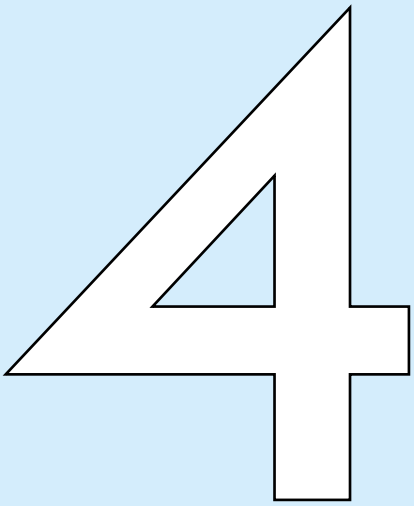
Účelem administrativních nástrojů je zajistit odpovídající přehled jednotlivých komponent KOUI. Tyto úzce souvisí s právní oblastí, zejména s ohledem na rámec možností výkonu činností, ke kterým je právní oblast zmocňuje, a rovněž i s oblastí institucionální, kdy jsou aplikovány prostřednictvím institucí zapojených do KOUI.

Informační a osvětové nástroje

Účelem informačních a osvětových nástrojů je zejména poskytnutí všech relevantních informací pro potřeby pochopení stanovených cílů rozvoje KOUI a jejich následného aktivního prosazování. Významné místo v osvětové oblasti mají vhodné formy ocenění aktivních subjektů za výsledky a přínos v oblasti KOUI.

Nástroje spolupráce

Z používaných forem na národní úrovni jsou významné zejména krátkodobé odborné akce a dlouhodobé platformy pro řešení speciálních problémů. S ohledem na požadavek zajistit průběžnou harmonizaci národního přístupu k řešení KOUI s přístupy v EU a NATO jsou účasti v pracovních komisích, výborech a skupinách zmíněných organizací k problematice KOUI významným přínosem při řešení problémů rozvoje KOUI.



Klíčové aktivity KOUI

Pro splnění výše uvedených strategických cílů v oblasti KOUI pro období do roku 2030 (a pro vývoj KP s výhledem do roku 2040) byly jako prioritní identifikovány tyto klíčové aktivity:

1.

Nastavení strategicky řízené a efektivně fungující KOUI

2.

Zvýšení kvality a důvěryhodnosti zajištění KOUI v ČR

3.

Podpora zajištění KOUI v ČR národními KP

4.

Cílená podpora rozvoje kryptologie a vývoje národních KP s využitím kapacit vědeckých a výzkumných pracovišť a komerční vývojové infrastruktury ČR

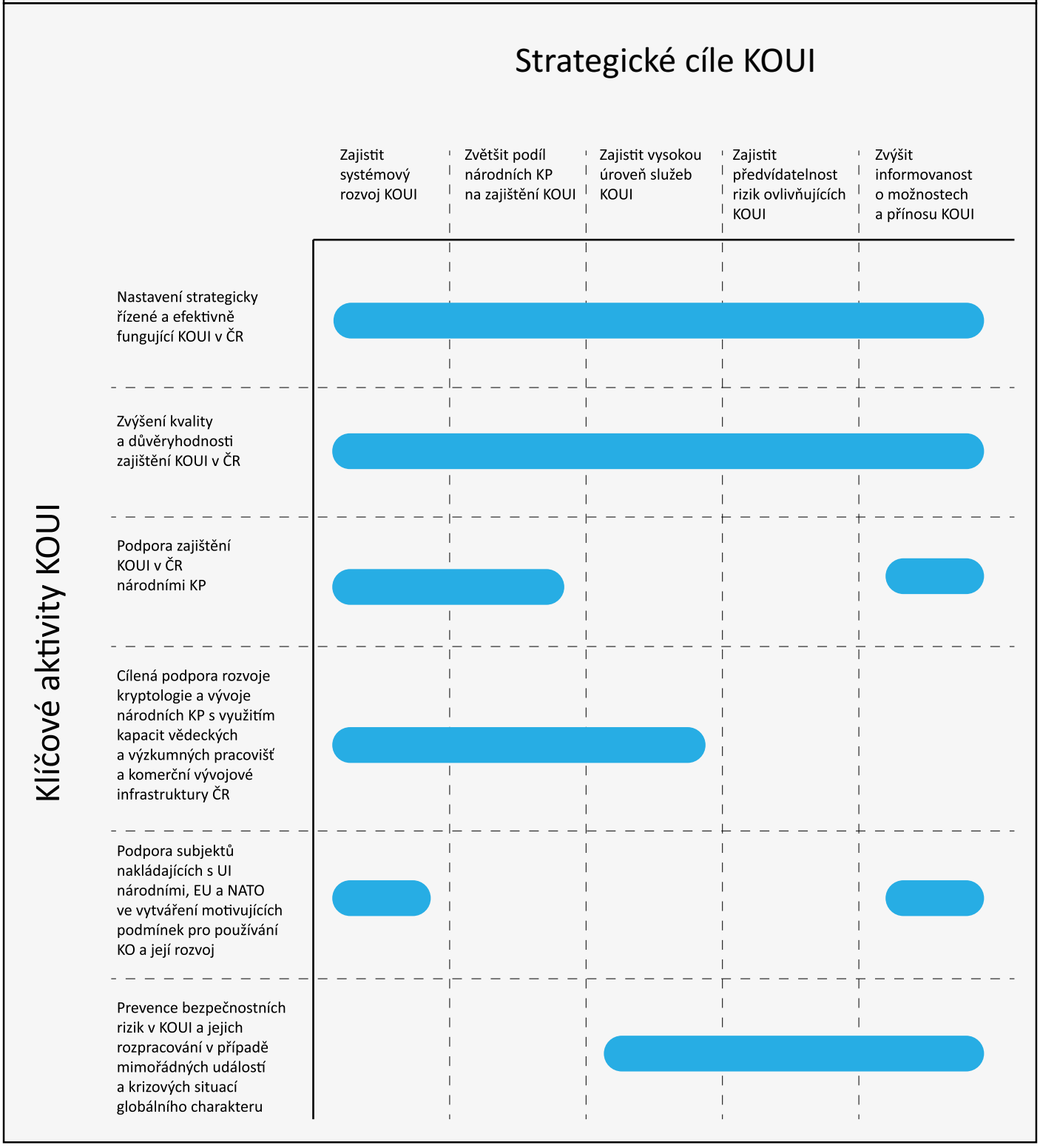
5.

Podpora subjektů nakládajících s UI národními, EU a NATO ve vytváření motivujících podmínek pro používání kryptografické ochrany a její rozvoj

6.

Prevence bezpečnostních rizik v KOUI a jejich rozpracování v případech mimořádných událostí a krizových situací globálního charakteru

Následující tabulka obsahuje přehled klíčových aktivit naplňujících jednotlivé strategické cíle.



4.1 Nastavení strategicky řízeného a efektivně fungujícího systému KOUI

Vytvořená KOUI v ČR, opírající se o ZoUI, není statická. Její aktuální podoba, funkčnost a účinnost se vyvíjí v čase a průběh je ovlivňován řadou lokálních a globálních faktorů.

Motiv:
Ovlivňující faktory aktuální podoby KOUI

Aktuální podoba KOUI je významně ovlivněna zejména mezinárodní situací, stavem národní legislativy a mezinárodními smlouvami, kterými je ČR vázána. Roli má též velmi dynamický rozvoj kryptologie a informačních technologií, jeho personální zajištění a v neposlední řadě stále rostoucí požadavky na množství UI a různorodost zařízení pro jejich zpracování. Aktuální podoba KOUI je dlouhodobě negativně ovlivňována úspornými rozpočtovými opatřeními ČR. V těchto složitých podmínkách je nutné, aby KOUI v ČR prošla řadou úprav, které spolu se základním požadavkem na bezpečnost UI zajistí také efektivní řízení a fungování všech jeho složek.

Cílový stav:
Právní ukotvení změn a systémové zajištění KOUI

Právně ukotvit změny v ZoUI, navazujících prováděcích předpisech a bezpečnostních standardech, které budou řešit aktuálně známé a předpokládané problémy zajištění KOUI v ČR. Navržená opatření musí prosazovat systémovost a předvídatelnost. Cílem je zajištění dostatečně širokých rámců a zmocnění pro všechny oblasti KOUI, aby byla v budoucnu minimalizována potřeba měnit ZoUI. Na podporu řešení problémů v KOUI je současně potřebné zapracování KOUI ve strategických bezpečnostních dokumentech ČR.

4.2 Zvýšení kvality a důvěryhodnosti zajištění KOUI

Konzistentní aktualizace nastavených opatření KOUI významnou měrou přispívají ke zvýšení úrovně poskytovaných bezpečnostních služeb a bezpečnostních záruk v rámci KOUI.

Motiv:
Aktualizace KOUI dle moderních požadavků

Upravit KOUI v ČR tak, aby odpovídala aktuálním požadavkům vyplývajících z rozvoje informačních technologií a kryptologie a stavu ekonomického a personálního zajištění. Současně musí být zajištěna požadovaná úroveň kvality souvisejících procesů a řešení odpovědnosti.

Cílový stav:
Zajištění důvěryhodnosti a kvality KOUI

V návaznosti na právně ukotvené změny v ZoUI a navazujících vyhláškách musí bezpečnostní standardy definovat opatření požadované úrovně kvality a zajištění odpovědnosti jednotlivých oblastí KOUI, aby všichni uživatelé využívající KOUI měli jistotu, že systém je ve všech jeho částech důvěryhodný. Soulad reálného a požadovaného stavu ve všech částech KOUI je pak kritériem při hodnocení účinnosti implementovaných opatření. Významným přínosem řešení se musí stát uplatňování otevřené a důvěryhodné komunikace mezi subjekty zajišťující KOUI.

4.3 Podpora zajištění KOUI v ČR národními KP

Zajišťování KOUI v národních KIS pomocí vlastních KP, které jsou vyvinuté, certifikované a vyráběné v ČR, je aktem svrchovanosti, kterým ČR vyjadřuje plnou kontrolu nad takovými KP.

Motiv:
Potřeba národních kryptografických prostředků

V současnosti je KOUI v národních KIS zajišťována převážně zahraničními KP, jejichž akvizice a provoz jsou spojeny s vysokými náklady. Využívání zahraničních KP rovněž zvyšuje závislost ČR na zahraničních dodavatelích a s tím spojená rizika v oblasti spolehlivosti a bezpečnosti dodavatelského řetězce. V ČR se sice vyvíjí a vyrábí národní KP, jejich rozvoj ale vyžaduje účinnou podporu ze strany státu. V aktuálních bezpečnostních dokumentech, které se týkají ochrany KOUI, není dostatečně zdůrazňována potřeba národních KP včetně jejich způsobilosti pro ochranu UI EU a NATO vyšších stupňů utajení, mj. s ohledem na bezpečnostní a strategický kontext a ekonomickou výhodnost.

Cílový stav:
Definování a podpora nasazování národních KP

V relevantních strategických dokumentech definovat kategorii národního KP jako jedné z forem naplňování zájmu státu v oblasti komunikační a informační bezpečnosti. Dle možností vývojového a výrobního potenciálu ČR musí být vytvářeny ze strany státu systémové podmínky pro nasazování a využívání těchto národních KP.

4.4 Cílená podpora rozvoje kryptologie a vývoje národních KP s využitím kapacit vědeckých a výzkumných pracovišť a komerční vývojové infrastruktury v ČR

V ČR se na problematiku teoretické a aplikované kryptologie zaměřuje řada vědeckých a výzkumných pracovišť a komerčních subjektů. Národním zájmem je nalezení efektivních forem spolupráce a využití kapacit těchto subjektů pro KOUI v ČR.

Motiv: Podpora teoretické a aplikované kryptologie

Zatímco téma teoretické kryptologie bylo donedávna doménou NÚKIB (a dříve Národního bezpečnostního úřadu), na aplikované kryptologii, zahrnující zejména vývoj KP, se dlouhodobě podílí i komerční subjekty. V obou těchto oblastech má nezastupitelné místo právě NÚKIB. Ten formou projektů a dílčím financováním podporuje jejich rozvoj, přičemž závěrečné výstupy hodnotí a schvaluje pro použití v KOUI.

Oblast teoretické kryptologie

V současné době je vývoj nových bezpečných základních kryptografických algoritmů (primitiv) velmi náročný proces, ve kterém mají rozhodující roli vědecký potenciál a řešitelské kapacity v oblasti kryptologie.

Dosavadní výsledky spolupráce, zejména NÚKIB s vědeckými a výzkumnými pracovišti formou projektů, vytváří dobrý základ, na kterém lze v následujícím období stavět. Současně je nutné upozornit, že širšímu zapojení vědeckých a výzkumných pracovišť v ČR do řešených úloh kryptologie brání rovněž neplnění podmínek pro přístup k UI.

Oblast vývoje KP

Národní vývoj KP v současných společenských a ekonomických podmínkách výrazně ovlivňují požadavky a směry rozvoje v kryptologii a informačních technologiích. Ty ukazují na potřebu změnit některé zaužívané přístupy a postupy v jeho zajištění.

U komerčních subjektů je vývoj KP vnímán jako ekonomicky nerentabilní. Důvodem je nedostatečná dotační politika ze strany zadavatelů vývoje KP, ale i státu. Praxe ukazuje, že v současnosti tyto dotace ani spolu se ziskem z následného prodeje zpravidla nepokrývají náklady vynaložené na vývoj KP.
Výrazný příznivý posun v oblasti dotační politiky by umožnil vývoj dalších národních KP a dílčích kryptografických modulů a vnesl by do vývoje systematičnost, jistotu a důvěru. Dalším motivačním prvkem pro subjekty vyvíjející KP by pak bylo nasazení těchto KP ve státní správě.

Cílový stav:

Podpůrná opatření pro rozvoj národní kryptografie

V návaznosti na právní rámec KOUI je nezbytné stanovit taková podpůrná opatření, která pro vědecká a výzkumná pracoviště zajistí zapojení do rozvoje národní kryptografie a pro komerční subjekty vytvoří důvěryhodné prostředí pro vývoj KP. Klíčovou roli v podpoře řešitelů má plán rozvoje národních KP, který sám je pro řešitele významným motivačním prvkem a zdrojem jejich dalšího odborného rozvoje. V rámci opatření mají své nezastupitelné místo vhodné formy ocenění a související osvětová a vzdělávací činnost. Cílem je vytvořit předpoklady pro neformální zájem o teoretickou a aplikovanou kryptologii.

4.5 Podpora subjektů nakládajících s UI při používání KOUI

Subjekty, které nakládají s UI, jsou povinny používat regulační rámce ZoUI. Při zpracování UI v KIS je národním zájmem, aby byla KO používána.

Motiv:

Potřeba rozšíření KOUI v digitální společnosti

Zajištění KOUI v KIS se v současnosti týká především státní správy, a to v oblastech obrany, bezpečnosti a zahraniční politiky. V ostatních oblastech státní správy a v komerční sféře je KOUI využívána ve velmi malém rozsahu. Další potřebu aplikace KOUI lze oprávněně očekávat zejména v souvislosti s prohlubující se digitalizací státu i společnosti. Právě rostoucí závislost společnosti na KIS s sebou přináší hrozby, které mohou výrazně ohrozit bezpečnost a funkčnost všech oblastí státu. Na to musí reagovat právě i opatření ve vztahu KOUI.

Cílový stav:

Informování a motivace subjektů k používání KOUI

Subjektům manipulujícím s UI poskytnout nejen informace o možnostech současné KOUI, ale rovněž je motivovat k jejímu používání. Cílem je zejména zvýšit odpovědnost a rozhodnost všech subjektů podílejících se na ochraně UI řešit problematiku KOUI včas, bezpečně, efektivně a odpovídajícím způsobem.

4.6 Prevence bezpečnostních rizik v KOUI a jejich rozpracování v případě mimořádných událostí a krizových situací globálního charakteru

Postupy pro řešení situací, které se vymykají běžným podmínkám zajišťování KOUI, jsou vždy součástí příslušné provozní dokumentace KP a KO. Tyto postupy musí odpovídajícím způsobem reagovat na současné a budoucí události, které mohou výrazným způsobem ovlivnit nastavené mechanismy zajištění KOUI.

Motiv:

Příprava na nestandardní události ohrožující KOUI

KOUI je v dnešní době ohrožena mnoha nestandardními událostmi, které mohou narušit průběh jejího zajištění.

ČR tak musí být připravena na zajištění KOUI v těchto případech použitím systémových opatření v personální, provozně technické a kryptologické bezpečnosti KOUI, a tím výrazně ovlivnit důsledky dopadů těchto událostí a v řadě případů jim také předcházet.

Cílový stav:

Zajištění funkčnosti a bezpečnosti KOUI během krizových situací

Zajistit funkčnost a bezpečnost KOUI během mimořádných událostí a krizových situací. Významnou součástí jsou preventivní opatření, která na základě vyhodnocení příznaků vzniku takových událostí spustí včas a v požadovaném rozsahu nastavené mechanismy s cílem maximálně eliminovat důsledky událostí na KOUI. Součástí opatření se musí stát plány obnovy a řešení KOUI v záložních KIS. Cílem je stanovit soubor opatření s důrazem na role a odpovědnosti lidského činitele, který bude podpořen právními předpisy a metodickými dokumenty.

5

Implementace a vyhodnocování naplnění NP KOUI

Předložená NP KOUI představuje realizovatelný a udržitelný směr, kterým by se KOUI měla ubírat.

Koordinace plnění těchto úkolů a prosazování myšlenek NP KOUI je úkolem NÚKIB. Jejich uvedení do života se však neobejde bez aktivní pomoci dotčených subjektů v KOUI a zajištění stabilního financování, a to i v současném náročném období optimalizace veřejných rozpočtů.

Uvedené cíle NP KOUI budou rozpracovány v dokumentu Implementační plán politiky kryptografické ochrany utajovaných informací v České republice, v němž budou obsaženy konkrétní, adresné a termínované úkoly. Implementační plán ve spolupráci s dotčenými subjekty zpracovává NÚKIB, který také koordinuje a pravidelně vyhodnocuje jeho plnění a informuje o něm Bezpečnostní radu státu.

Dokument NP KOUI upravuje zajištění a rozvoj KOUI v souladu s nastavenými cíli na období do roku 2030 s výhledem do roku 2040. Případné požadavky na změny a doplnění NP KOUI lze uplatňovat u NÚKIB, který je po projednání s kladným závěrem zpracuje do podoby návrhu aktualizace NP KOUI.

Úspěšné naplňování cílů a prioritních aktivit NP KOUI může být ohroženo následujícími faktory:

1. Včas neschválené požadované právní úpravy k realizaci NP KOUI, zejména v ZoUI a navazujících vyhláškách.

2. Nedodržování stanovených postupů a opatření v NP KOUI.

3. Nedostatečná informovanost subjektů zúčastněných v zajišťování KOUI o prioritách, cílech a opatřeních NP KOUI a nedostatečná podpora realizace NP KOUI z jejich strany.

4. Neschválení dokumentu Implementační plán politiky kryptografické ochrany utajovaných informací v České republice, který rozpracovává NP KOUI do podoby konkrétních úkolů, případně neplnění těchto úkolů.

5. Absence potřebných zdrojů, především lidských a finančních, pro naplňování NP KOUI.

Reference

Právní předpisy

[1]	Zákon č. 239/2000 Sb., o integrovaném záchranné systému a o změně některých zákonů, ve znění pozdějších předpisů.
[2]	Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.
[3]	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[4]	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
[5]	Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor ve znění vyhlášky č. 453/2011 Sb.
[6]	Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací ve znění vyhlášky č. 434/2011
[7]	Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků ve znění pozdějších předpisů
[8]	Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací ve znění vyhlášky č. 417/2013
[9]	Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů.

Ostatní dokumenty

[11]	Analýza stavu kryptografické ochrany utajovaných informací v České republice 2023, NÚKIB, čj. V41/2024/K-NÚKIB-I/410 (utajovaný dokument).
[12]	Bezpečnostní strategie České republiky 2023. [online]. [cit. 14. 12. 2023]. Dostupné z https://vlada.gov.cz/assets/ppov/brs/dokumenty/Bezpecnostni_strategie_2023.pdf.
[13]	Obranná strategie České republiky, schválila vláda ČR dne 4. října 2023. [online]. [cit. 2. 9. 2024]. Dostupné z https://mocr.army.cz/images/id_40001_50000/46088/obranna__strategie-_c_r_2023_final.pdf
[14]	Rozhodnutí Rady EU ze dne 23. září 2013, o bezpečnostních pravidlech na ochranu utajovaných informací EU, 2013/448/EU. [online]. [cit. 14. 12. 2023]. Dostupné z https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32013D0488
[15]	Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti, Rada Evropské unie, 7371/22, Brusel 21. března 2022. [online]. [cit. 14. 12. 2023]. Dostupné z https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/cs/pdf
[16]	Security within the North Atlantic Treaty Organisation (NATO), C-M(2002)49-REV1, [online]. [cit. 14. 12. 2023]. Dostupné z https://nbu.gov.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/
[17]	NATO 2022 Strategic Concept, NATO Summit in Madrid, 29 June 2022. [online]. [cit. 2. 9. 2024]. Dostupné z https://www.nbu.cz/download/C-M_2002_49_REV1_znackaNBU.pdf
[18]	Post-Quantum Cryptography, Selected Algorithms 2022. [online]. [cit. 2. 9. 2024]. Dostupné z https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
[19]	Metodika přípravy veřejných strategií. [online]. [cit. 2. 9. 2024]. Dostupné z https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022